



SPYWOLF

Security Audit Report



Completed on
January 24, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **OxPad** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Vulnerability Check	05
Threat Levels	06
Found Threats	07-A/07-C
Good Practices	08
Tokenomics	09
Team Information	10
Website Analysis	11
Social Media & Online Presence	12
About SPYWOLF	13
Disclaimer	14



OxPad



PROJECT DESCRIPTION

According to their whitepaper:

Oxpad is a hybrid fundraiser fusing marketing along an innovative borrow mechanism to raise funds for startups, guarantee returns for investors, in addition to introducing the CBC standard and offering a suite of products including a fundraiser, swap, liquidity staking and a marketing accelerator.

Release Date: Presale starts in February 1st, 2023

Category: Launchpad



CONTRACT INFO

Token Name
ZeroXPad

Symbol
ZXP

Contract Address

0x15153e3Cfa74fd82e5f0cE6D16ce3f250D89d978

Network

Binance Smart Chain

Language

Solidity

Deployment Date

Jan 24, 2023

Verified?

Yes

Total Supply

10,000,000

Status

Not launched

TAXES

Buy Tax

3%

Sell Tax

3%

*Fees can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of January 22, 2023)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
No limit

DEX
PancakeSwap

LP Address(es)

Liquidity not added yet



TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	10000000 ZXP
Median Transfer Amount	10000000 ZXP
Average Transfer Amount	10000000 ZXP
First transfer date	2023-01-24
Last transfer date	2023-01-24
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-01-24 17:29:27 UTC
Created	2023-01-24 17:29:27 UTC
Create TX	0xbbee4e892bb06050d8b2a20307e9b4ef0d55c896da808c2fd5fd60c49ab7a266
Creator	0x488a8ca56f29bfbe28e6f4cf898d5c3c1455deda



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



Informational

Owner can set buy fees up to 3% and sell fees up to 24% (until disableProtection function is triggered).

Once disableProtection function is triggered sell fees can be set up to 3%.
Combined buy+sell = 27%.

```
function setBuyFee(uint256 buyFee) public onlyOwner {
    require(
        buyFee > 0 && buyFee < 300,
        "0xPad: buy fee must be between 0 and 300"
    );
    buyFee_ = buyFee;

    emit BuyFeeChanged(buyFee);
}

function setSellFee(uint256 sellFee) public onlyOwner {
    require(
        sellFee > 0 && sellFee < 300,
        "0xPad: buy fee must be between 0 and 300"
    );
    sellFee_ = sellFee;

    emit SellFeeChanged(sellFee);
}

function disableProtection() public onlyOwner {
    require(
        protectionEnabled_,
        "0xPad: sell protection is already disabled"
    );
    protectionEnabled_ = false;

    emit ProtectionDisabled();
}

function _transfer(address from,address to,uint256 amount) internal virtual override {
    .....
    if (protectionEnabled_) {
        uint256 penaltyPercentage = sellFee_.add(
            sellFee_.mul(protectionModifier_)
        );

        fees = amount.mul(penaltyPercentage).div(10000);
    }
    .....
}
```



Informational

Owner can exclude address from fees.

```
function excludeFromFees(address holder) public onlyOwner {
    require(
        holder != address(0),
        "0xPad: holder can not be a null address"
    );
    isExcludedFromFees_[holder] = true;
}

function includeInFees(address holder) public onlyOwner {
    require(
        holder != address(0),
        "0xPad: holder can not be a null address"
    );
    isExcludedFromFees_[holder] = false;
}
```

Owner can set multiplier for sell fees up to x7 until disableProtection() function is triggered.

```
function setProtectionModifier(uint256 protectionModifier)
    public
    onlyOwner
{
    require(
        protectionModifier > 0 && protectionModifier <= 7,
        "0xPad: protection modifier must be greater than 0 and less than 7"
    );
    protectionModifier_ = protectionModifier;

    emit ProtectionModifierChanged(protectionModifier);
}
```



Informational

Important!

Owner is not excluded from any restrictions by default. In order to add the initial liquidity – trading must be enabled and taxes must be set to 0 and/or the address which will add the initial liquidity to be excluded from fees. If the above procedure is not applied tokens will be deducted from the liquidity adding address and transferred to treasury address. This will impact the initial token's price and might lead to unexpected rates.



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

0xPad

GOOD PRACTICES FOUND

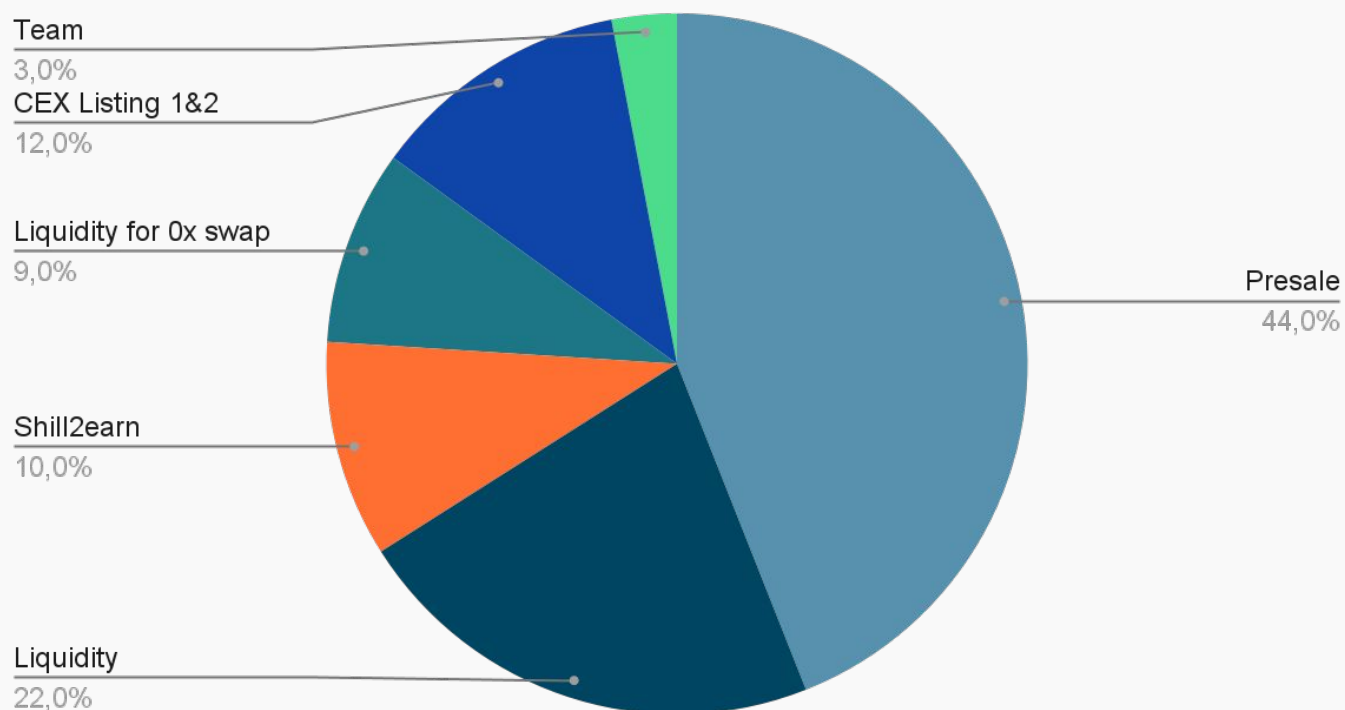
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot stop or pause the contract
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



*The following tokenomics are based on the project's whitepaper and/or website:

- 44% - Presale
- 22% - Liquidity
- 10% - Shill2earn
- 9% - Liquidity for 0x swap
- 12% - CEX Listing 1&2
- 3% - Team

Tokens distribution



TOKENOMICS



THE TEAM

! The team is anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://www.0xpad.app/>

Domain Registry

<https://www.godaddy.com>

Domain Expiration

Expires on 2024-01-14

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Single page design,
appropriate color scheme
and graphics.

Content

The information helps new
investors understand what
the product does right away.

No grammar mistakes found

.

Whitepaper

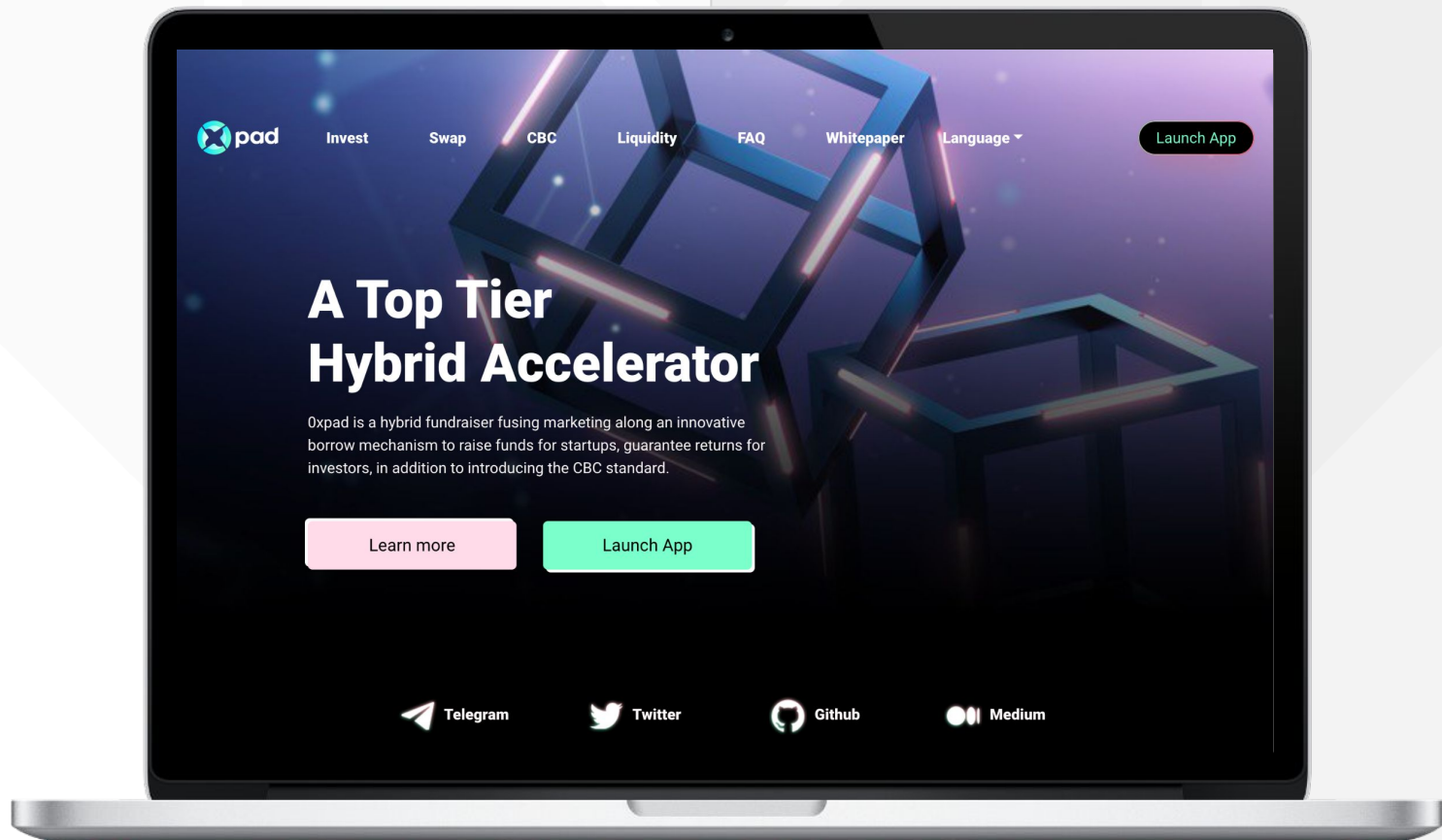
Well written, explanatory.

Roadmap

Yes, goals set with time
frames.

Mobile-friendly?

Yes



0xpad.app

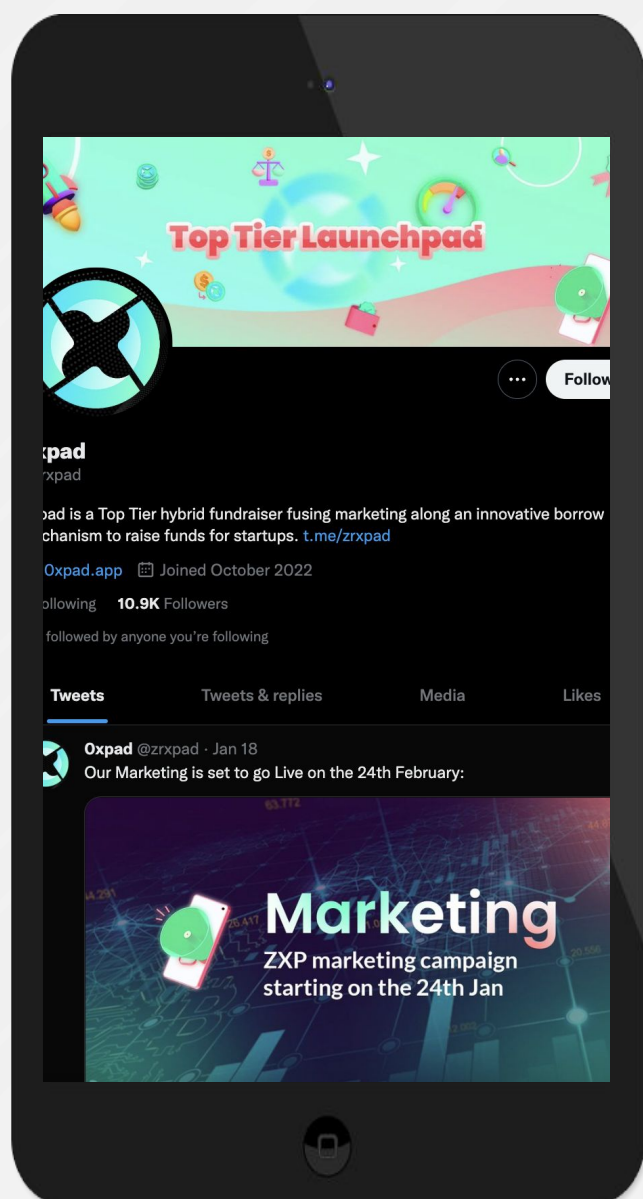


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

Project's social media channels are active.



Twitter

@zrxpad

- 10 600 followers
- Active
- Posts frequently



Discord

- Not available



Telegram

@zrxpad

- 9 764 members
- Few active members
- Active mods



Medium

@zrxpad

- 5 articles



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[SPYWOLF.NETWORK](https://spywolf.network)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFOFFICIAL](https://t.me/SPYWOLFOFFICIAL)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://github.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.